UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

FILED
APR 09 2024
PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY _____ DEP CLK

IN THE MATTER OF THE SEARCH OF: FILES CONTAINED WITHIN THE NCMEC CYBERTIPLINE REPORTS 165595919, 165555994, 165764573, AND 166247652 CURRENTLY IN THE CUSTODY OF THE ARMED FORCES INTERNET CRIMES AGAINST CHILDREN (ICAC) TASK FORCE AND MORE FULLY DESCRIBED IN ATTACHMENT A, ATTACHED HERETO.

Case No. 7:24-mj-1079-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Files contained in the NCMEC Cybertips 165595919, 16555994, 165764573, 166247652 as described in Attachment A

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment (insert) hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Distribution, Receipt, and/or Possession Child Pornography
18 U.S.C. § 2252	Distribution, Receipt, and/or Possession Child Pornography

The application is based on these facts:
See attached affidavit which is attached hereto and incorporated herein by reference

☑ Continued on the attached sheet.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

HALL.MICHAEL.SHANNON.II.1298030698 Digitally signed by HALL.MICHAEL.SHANNON.II.1298030698 Date: 2024.04.03 16:23:59 -04'00'

Applicant's signature

Michael S. Hall II, Special Agent

Printed name and title

On this day, Michael Hall appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Application for a Search Warrant.

Date: April 9 2024

Judge's signature

City and state: Wilmington, North Carolina

Robert B. Jones, Jr., United States Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH OF: FILES CONTAINED WITHIN THE NCMEC CYBERTIPLINE REPORTS 165595919, 165555994, 165764573, AND 166247652 CURRENTLY IN THE CUSTODY OF THE ARMED FORCES INTERNET CRIMES AGAINST CHILDREN (ICAC) TASK FORCE AND MORE FULLY DESCRIBED IN ATTACHMENT A, ATTACHED HERETO.	Case No. 7:24-MJ-1079-RJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Michael Hall, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief.

INTRODUCTION

1. I am a Special Agent (SA) with the Naval Criminal Investigative Service, and have been employed since 2021. I am assigned to the Family and Sexual Violence Squad at Carolinas Field Office in Camp Lejeune, North Carolina. I regularly investigate felony crimes having a Department of the Navy nexus, to include, but not limited to, death investigations, adult and child sexual assaults, domestic and aggravated assaults, child abuse, child exploitation, and child sexual abuse material (CSAM) investigations. I graduated from the Criminal Investigator Training Program,

and NCIS Special Agent Basic Training Program at the Federal Law Enforcement Training Center (FLETC). I received training in various topics, including but limited to: constitutional and criminal law, operational activities, physical tactics, behavioral sciences, use of force, and ethics and core values. Prior to graduating from FLETC, I served as a Marine Special Agent (MSA) with NCIS from November 2019 to September 2021. I am a member of the NCIS Carolinas Field Office Major Case Response Team (MCRT), wherein I have had multiple opportunities to participate in search warrants and command authorizations for search and seizures as part of felony level criminal investigations. Additionally, I have participated in the performance of my duties in the successful seizure of both physical and electronic/digital evidence. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices and the Internet). Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This affidavit is submitted in support of an application for a search warrant for the file(s) submitted in connection with CyberTipline Reports 165595919, 165555994, 165764573, and 166247652 (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5).

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A are located in the place described in Attachment A. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or

foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or

foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

e. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or

that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

CYBERTIPLINE REPORTS

6. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children and serves as a repository for information about child pornography. Federal law requires NCMEC to operate the CyberTipline and requires Electronic Service Providers ("ESP") to report apparent instances of child pornography offenses. Providers also have the discretion to submit reports concerning planned or imminent child pornography

offenses. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or "CyberTip"). The Electronic Service Provider submits the report and uploads content to NCMEC via a secure connection. Aside from required information such as incident type, date, and time, reporters can also fill in voluntary reporting fields such as user or account information, IP addresses, or information regarding the uploaded content itself, as well as other information it may have collected in connection with the suspected criminal activity. The Electronic Service Provider may or may not independently view the content of the file(s) it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the Electronic Service Provider submits, such as IP addresses. NCMEC then packages the information from the Electronic Service Provider along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is believed to have occurred. Based on U.S. v. Ackerman, every file reported to NCMEC must have either been viewed by the reporting ESP or publicly available, in order for Law Enforcement to view the files. Otherwise, a search warrant is required in order to view the file(s).

PROBABLE CAUSE

7. On or about July 01, 2023, the ESP, Google, Inc., submitted Cyber Tipline Report 165555994 to NCMEC. As reported by the ESP, the incident type was: Child Pornography (possession, manufacture, and distribution), and the incident date

and time were listed as: July 01, 2023, 02:17:13 UTC. Furthermore, the CyberTip listed the incident type as: Apparent Child Pornography and noted the Report contained a "Hash Match."

8. On or about July 03, 2023, the ESP, Google, Inc., submitted Cyber Tipline Report 165595919 to NCMEC. As reported by the ESP, the incident type was: Child Pornography (possession, manufacture, and distribution), and the incident date and time were listed as: July 03, 2023, 02:25:18 UTC. Furthermore, the CyberTip listed the incident type as: Apparent Child Pornography and noted the Report contained a "Hash Match."

9. On or about July 06, 2023, the ESP, Google, Inc., submitted Cyber Tipline Report 165764573 to NCMEC. As reported by the ESP, the incident type was: Child Pornography (possession, manufacture, and distribution), and the incident date and time were listed as: July 06, 2023, 06:42:31 UTC. Furthermore, the CyberTip listed the incident type as: Apparent Child Pornography and noted the Report contained a "Hash Match."

10. On or about July 13, 2023, the ESP, Google, Inc., submitted Cyber Tipline Report 166247652 to NCMEC. As reported by the ESP, the incident type was: Child Pornography (possession, manufacture, and distribution), and the incident date and time were listed as: July 13, 2023, 08:00:51 UTC. Furthermore, the CyberTip listed the incident type as: Apparent Child Pornography and noted the Report contained a "Hash Match."

11. The reports indicated neither the ESP nor NCMEC conducted a review of the contents of the file(s). The ESP reported the uploads were associated with the following additional information: Full name: "Daniel Bradley," email address "danielbradley123456@gmail.com," phone number 770-317-4363, date of birth 11-12-2002. The ESP additionally provided twenty-one (22) Internet Protocol (IP) addresses associated with the Google user's upload and/or login dates, as early as July 01, 2023, and as recent as October 07, 2023.

12. NCMEC then used publicly available search tools to query the IP addresses and determined six (6) IP addresses resolved to Charlotte, NC, four (4) IP address resolved to Jacksonville, NC, one (1) IP address resolved to Raleigh, NC, one (1) IP address resolved to Fort Mill, SC, and one (1) IP address resolved to Easley, NC. NCMEC additionally conducted a query of the phone number provided by the ESP, 770-317-4363, which resolved to Verizon Wireless. Upon receipt of the CyberTip, I conducted an additional query of the aforementioned phone number and identified LCpl Daniel BRADLEY ("BRADLEY"), USMC, 8th Communications Battalion, 2nd Marine Expeditionary Force, as being associated with the phone number. Law enforcement queries confirmed BRADLEY was an Active-Duty Marine stationed at Camp Lejeune, NC. I currently have access to the CyberTipline Report and the contents of the file the ESP uploaded in connection with the CyberTip through the ICAC Data System (IDS).

13. I know from my training and experience the ESP flags and reports images or files that have the same "hash values" as images that have been reviewed

and identified by NCMEC or by law enforcement as child pornography. A hash value is akin to a fingerprint for a file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

14. Here, I know from my training and experience the ESP compares the hash values of files that its customers transmit on its systems against the list of hash values the Armed Forces Internet Crimes Against Children (ICAC) Task Force has. If the ESP finds that a hash value of a file on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the ESP's systems.

15. Therefore, there is probable cause to believe the content of the file(s) the ESP reported in connection with the submitted CyberTipline Reports 165595919, 165555994, 165764573, and 166247652 contain at least one image or video file of previously-identified child pornography.

LEGAL AUTHORITY

16. The legal authority for this search warrant application is derived from Title 18, United States Code, chapter 121, §§ 2701-11, entitled, "stored wire and electronic communications and transactional records access."

17. Title 18 United States Code 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction.

18. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of North Carolina because IP subscriber information indicated that the subject of the CyberTipline Reports 165595919, 165555994, 165764573, and 166247652, uses the account from an address within the Eastern District of North Carolina. See 18 U.S.C. § 3237(a); see also 18 U.S.C. §§ 3231 and 3232.

CONCLUSION

19. Based on the investigation described above, probable cause exists to believe inside the file the ESP uploaded in connection with the above Cyber Tipline Reports (described in Attachment A), will be found evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Sections 2252(a)(1), (2), (4) and 2252A(a)(1), (2), (3), and (5) (described in Attachment B).

instrumentalities of a violation of Title 18, United States Code, Sections 2252(a)(1), (2), (4) and 2252A(a)(1), (2), (3), and (5) (described in Attachment B).

20. I, therefore, respectfully request that that attached warrant be issued authorizing the search and seizure of the items described in **Attachment A** and listed in **Attachment B**.

HALL.MICHAEL.SHANNON.II.1298030698 Digitally signed by HALL.MICHAEL.SHANNON.II.1298030698 Date: 2024.04.05 08:50:10 -04'00'

Michael S. Hall II, Special Agent,
Naval Criminal Investigative Service

Sworn to via telephone after submission by reliable electronic means, pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3), this 9 day of April 2024.

ROBERT B. JONES, JR.
UNITED STATES MAGISTRATE JUDGE